



# **Qualys Multi-Vector EDR**

## **Lab Tutorial Supplement**

Table of Contents

EDR ACTIVATION AND SETUP.....3

INVESTIGATE EVENTS AND INCIDENTS.....8

HUNT FOR SUSPICIOUS ACTIVITY ..... 13

PERFORM REMEDIATION ACTION..... 18

CONFIGURE RULE BASED ALERTS ..... 19

CORRELATE PREVENTION ACROSS MULTIPLE VECTORS..... 20

EDR CERTIFICATION EXAM..... 24

# EDR Activation and Setup

To successfully install and use Qualys EDR in your environment, the following configuration steps are required:

1. Install the Qualys Cloud Agent on target host
2. Assign the target agent host to an EDR enabled Cloud Agent Configuration Profile
3. Activate EDR for the target agent host (If EDR is not enabled in the Cloud Agent activation key)

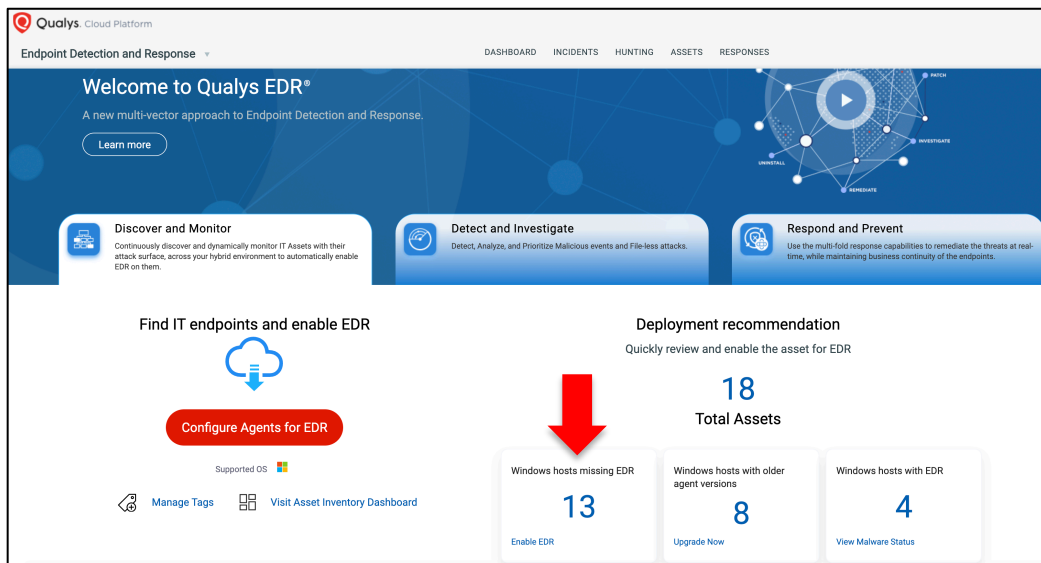
When Asset Tags are strategically used for host assignment, step 2 (listed above) can potentially be performed prior to agent installation (step 1).

## Identify Assets Missing EDR

Endpoint security starts with visibility. The EDR application automatically identifies agent hosts that do not have EDR enabled and hosts running older version of the Cloud Agent.

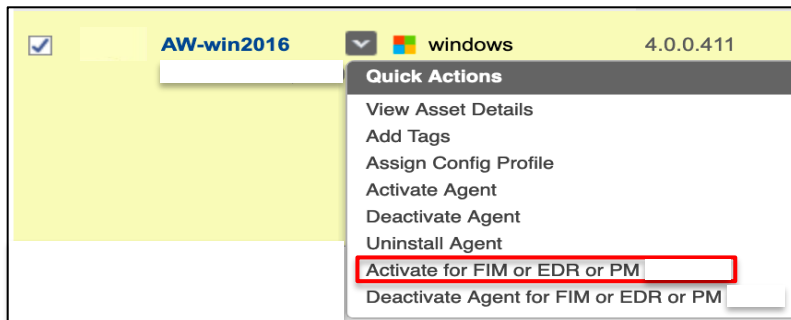
You can find such assets on the EDR Welcome page under the “Discover and Monitor” section.

The “Windows hosts missing EDR” widget identifies agent hosts that do not have EDR enabled and the “Windows hosts with older agent versions” widget identifies hosts running Cloud Agent version lower than 4.0.0.



## Activate EDR Module

You can activate EDR on agent assets from the agent “Quick Actions” menu.



Simply select the “Activate for FIM or EDR or PM” option to enable EDR for a given asset. Alternately you can also use Cloud Agent APIs to activate EDR in bulk across multiple agent assets.

## Integrated Anti-Malware Protection

Qualys Multi-Vector EDR now includes integrated antimalware detection capabilities, providing additional real-time protection against the latest threats. This convergence of Malware Protection Products with Endpoint Detection & Response (EDR) delivers comprehensive protection against known and unknown threats.

Key capabilities include:

- **On-access protection:** prevents new malware threats from entering the system by scanning local and network files when they are accessed (opened, moved, copied or executed), boot sectors, and potentially unwanted applications (PUA).
- **On-demand scanning:** scans the file system and memory for malware and other threats and takes remediation actions
- **Behavioral-based protection:** operating on a zero-trust assumption, Qualys Malware Protection can monitor active applications and processes for any signs of malicious behavior. It relies on actual behavior characteristics instead of signatures or binary or code fingerprints. This allows Qualys Malware Protection to consistently detect new ransomware variants, other zero-day threats, and file-less attacks
- **Network and Traffic Protection:** prevents malware from being downloaded to the endpoint by scanning incoming emails and web traffic in real-time. In addition, protect against attack techniques used to gain access to specific endpoints, such as brute-force attacks, network exploits, and password stealers.

- **Phishing Protection:** Automatically block known phishing web pages to prevent users from inadvertently disclosing private or confidential information to online fraudsters.

Malware detection events captured on the agent host can be viewed and analyzed from the Qualys Cloud Console, allowing customers to enrich malicious events with contextual event data collected by Qualys EDR.

## Configuration Profile

EDR host assets must belong to a Configuration Profile with the “EDR” module enabled.

The screenshot shows the 'Configuration Profile Edit' interface. On the left is a sidebar with 'Edit Mode' and various modules like General Info, Blackout Windows, Performance, Assign Hosts, Agent Scan Merge, VM Scan Interval, PC Scan Interval, SCA Scan Interval, FIM, EDR (selected), and PM. The main area is titled 'Endpoint Detection and Response'. It contains a toggle switch 'Enable EDR module for this profile' which is turned ON. Below this is a 'Configuration' section with a note: 'These settings define operational setting for the agent'. It includes three settings: 'Max event log size\*' with a value of 1024 KB (range 10 - 10240), 'Payload threshold time\*' with a value of 60 secs (range 30 - 1800), and 'Maximum disk usage for EDR Data\*' with a value of 1024 MB (range 500 - 5120). At the bottom of this section is another toggle switch 'Enable Malware Protection for this Profile' which is also turned ON. At the very bottom of the window are 'Cancel' and 'Save' buttons.

Ensure the “Enable EDR module for this profile” switch is in the “ON” position.

**Max event log size** – EDR events are transmitted to the Qualys Cloud platform when the EDR event log file reaches the maximum specified size. You can specify a file size between 10 KB and 10240 KB. Default is 1024 KB. This value can be lower if the Payload threshold time is lower.

**Payload threshold time** – EDR events are transmitted to the Qualys Cloud platform when the EDR payload threshold time is hit, i.e., the specified seconds elapse after the previous payload was sent to the Qualys Cloud Platform. You can specify a threshold between 30 seconds and 1800 seconds. Default is 60 seconds. This value is lower the better to prevent data loss on busy systems.

**Maximum disk usage for EDR Data** – This is the maximum size on disk available to a Cloud Agent for caching EDR events to be sent to the Qualys Cloud Platform for processing. If the maximum size is reached, the oldest events are deleted in order to

create space for newly generated events. You can specify a disk usage size between 100 MB and 2048 MB. Default is 1024 MB.

**Navigate to the following URL to view the “EDR Activation and Setup” tutorial:**



<http://ior.ad/7fE0>

**Enable Malware Protection for this Profile** – If your Qualys account has the Integrated Malware Protection feature enabled, you can enable this feature in the Cloud Agent profile to install Malware Protection on your agent host.

## AV Profile

For agent hosts with the Malware Protection feature enabled in the configuration profile, the EDR manifest is installed on the agent host with Qualys Malware Protection’s integrated set of basic virus definitions. The Malware Protection module starts updating the latest virus definitions as soon as it is installed. As the virus definitions are downloaded on the endpoint, the Default antivirus configuration as shown below is also downloaded on the endpoint asset.

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes 'Endpoint Detection and Response' and a 'CONFIGURATION' tab. The main content area is titled 'Configuration' and shows a search bar and a table of AV profiles. The table has columns for Profile Name, Description, Active on Assets, On Access Scan, On Demand Scan, Behavioral, Network Protection, Network Attack Defense, Created By, and Last Updated. The 'Default' profile is listed with a description of 'default profile for all assets' and various settings.

PROFILE NAME	DESCRIPTION	ACTIVE ON ASSETS	ON ACCESS SCAN	ON DEMAND SCAN	BEHAVIORAL	NETWORK PROTECTION	NETWORK ATTACK DEFENSE	CREATED BY	LAST UPDATED
Default DEFAULT	default profile for all assets	16	Disabled	Not Scheduled	Disabled	Disabled	Disabled	System	20 hours ago

You can view and edit the Default AV (anti-virus) Profile from under the “CONFIGURATION” tab to enable required Malware Protection features for the agent host. The agent will receive the changes through an updated EDR manifest.

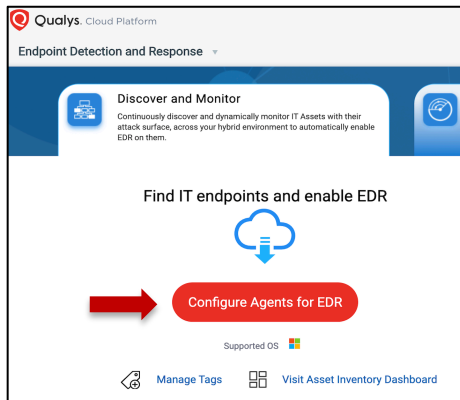
**Navigate to the following URL to view the “Malware Protection Activation and Setup” tutorial:**



<https://ior.ad/7T0A>

# Upgrade Multiple Agent Activation Keys

Within the EDR application, you can upgrade multiple Cloud Agent Activation Keys to use EDR. On the EDR welcome page, simply click “Configure Agents for EDR” and then select one or more agent keys to upgrade. All the agents associated with the activation key/keys will be upgraded and enabled for EDR.



**Navigate to the following URL to view the “Upgrade Agent Activation Keys” tutorial:**



<http://ior.ad/7gh9>

## View Assets

The “Assets” section in the EDR application contains list of agent host assets with the EDR and Malware Protection modules activated. Here you can get up-to-date views on a selected asset's details, its events, and incidents in one place.

For agent hosts with the Malware Protection feature enabled in the agent configuration profile, the AV status is updated to “Installed Functioning” after the module is installed and the latest anti-virus definitions are downloaded on the host.

NAME	OPERATING SYSTEM	AGENT VERSION	LAST CHECKED IN	CREATED ON	AV STATUS	LAST LOGGED IN USER
win8hq01 fe80:0:0:0:bf:d572:a0db:2596, 10.46.10...	Microsoft Windows Embedded 8.1 Industry Pr...	4.6.1.6	Nov 05, 2021	Sep 01, 2021	Installed Functioning	qualys
win2k12-65-53	Microsoft Windows MultiPoint Server 2012 St...	4.3.1.107	Nov 05, 2021	Apr 14, 2021	-	WmsShell

# Investigate Events & Incidents

Qualys Cloud Agents collect file, process, mutex, network, and registry events from their hosts. An incident may be comprised of multiple events associated with the detected malware.

## EDR Events

An “object” is an artifact on the system, without state information. The agent collects data for 5 types of objects:

- **File** – Portable Executable (PE) and non-PE files (PDF, XLS, PPT, etc.) on local attached disks (called “image”)   
PE is a file format for executables, object code, DLLs and others used in 32-bit and 64-bit versions of Windows operating systems. It is used for EXE, DLL, SYS (device driver) and other file types. Agent collects data for both user files and kernel files.
- **Process** – a running process, usually from an image
- **Process Network Connection** – a network state of a process
- **Mutex** – Mutant Handle, a shared memory resource used by processes
- **Registry** – Windows, locations used for persistence (auto-start)

Actions and events on the object include state information. The agent collects data about various objects and associated actions on the object in real-time. You can see information about objects along with their state in the EDR application.

An object with its state information includes:

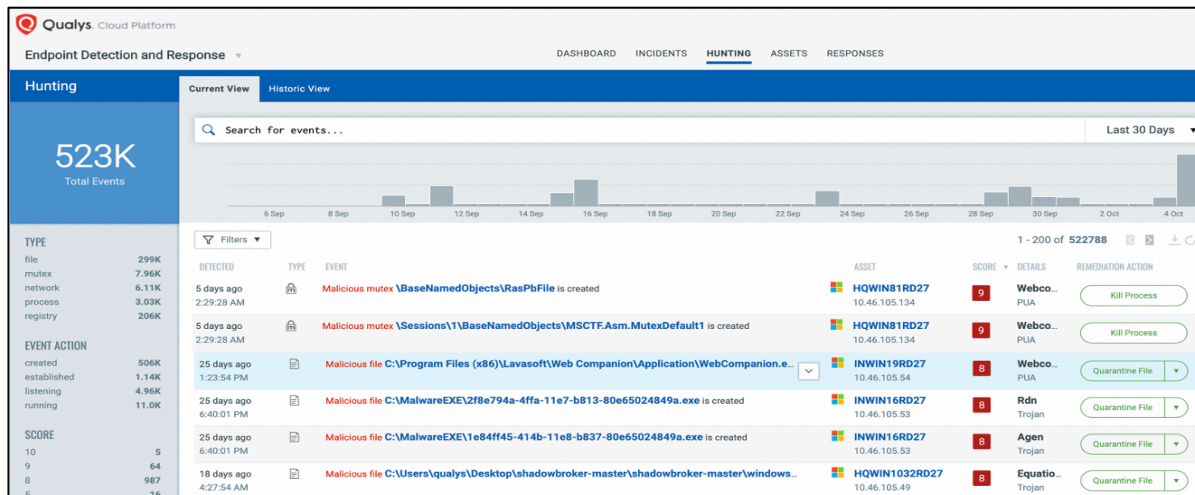
- File  
Created | Deleted | Renamed | Write
- Process  
Running | Terminated
- Mutex  
Running | Terminated
- Network  
Established | Closed | Listening



- Registry  
Created | Deleted



## Hunting section

You can see information about objects along with their state in the EDR app under the “Hunting” section.



You can filter and search for malicious file, process, mutex and network related events. This way, you reduce potentially thousands of events, to the few that matter. You can group events by event Type (file, process, mutex and network), Action (file creation, network connection established or listening, process running or terminated, etc.) and event Score and perform remediation actions.

Simply use the “Quick Actions” menu of an event, to select the “Event Details” option

← Event Details	
<b>Malware</b>	
Score	9 <span>Mutex for a Malicious Process</span>
Family	Webcompanion
Category	PUA
<b>Event</b>	
ID	M_5b1da240-8753-4218-a1e4-b4cec48670ed_282484113218700286_1356
Event Collected Date	Oct 9, 2020 11:16 PM
Object Type	MUTEX
<b>Handle</b>	
Handle Action	RUNNING
Handle Name	\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Handle Type	Mutant
<b>Image</b>	
Image Name	C:\Program Files (x86)\Lavasoft\Web Companion\Application
Image Full Path	C:\Program Files (x86)\Lavasoft\Web Companion\Application\Lavasoft.WCAssistant.WinService.exe
MD5	7faaf139ca5919e9970b5bc98ec1422 
SHA256	1205d3b4feccd8ef5aafd15be85fe05f84f2f831f7d8f668db4b4e5be2ba14581 

The “Event Details” page displays details such as image path, associated user, process ID, MD5/SHA256 hash value, etc. about the object (file/process/mutex/network connection) and the object state (file created, process/mutex running or terminated, network listening on a port, network connection established).

## Event Score

The Qualys EDR detection and scoring engine natively correlates all event telemetry data to commercial threat feed and research from Qualys Malware Labs and assigns each event and asset, a score between 0 to 10. The scoring system is dependent on the object type associated with the event and the threat perception.

An event with score 0 is a non-malicious event. An event with a score 1 indicates that a remediation\corrective action was performed on the event, and it is no longer a threat. Scores between 2 to 10 indicate malicious behavior related to file, process, or network activity with varying confidence levels.

Scores between 2 to 4 indicate malicious events at a low confidence level, 5 to 7 indicate malicious events at a medium confidence level and scores between 8 to 10 indicate confirmed malicious events with a high confidence score.

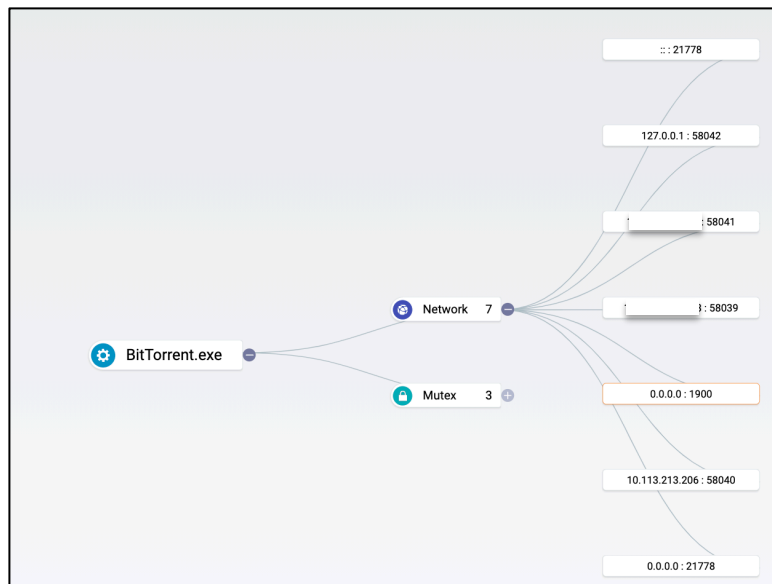
These scores assist incident responders to prioritize their response actions.

## Event Relationship Tree

On the “Event Details” page, you can see the event relationship tree which helps you visualize how a malicious object is tied to other objects on the asset which provides better context for understanding the attack chain. As with all things hunting, context is important, and we can often get more context by looking at the parent and children of processes.

An event of “Process” type will show its parent and child processes along with the mutex and network connection of the process.

For the event of Network type, you see network connection of a process and for the event of Mutex type, mutex connection of a process.



This information is useful for proactive threat hunting and for analysis during a post-breach investigation.

**Navigate to the following URL to view the “EDR Events” tutorial:**



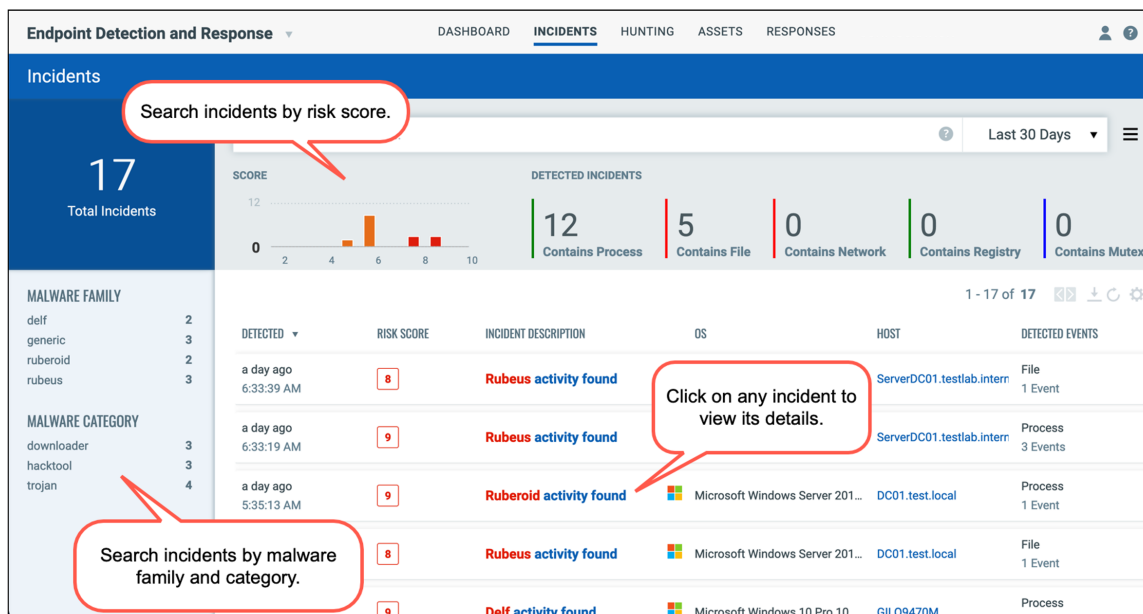
<https://ior.ad/7EJN>

## EDR Incidents

An EDR Incident is comprised of one or more events that are related to one another, as part of a detected malware infection or host compromise.

An Incident can consists of one of more File, Process, Mutex, Network, or Registry events. The “Incidents” section contains the list of all active incidents in your environment.

A summary of the total number of detected event types is provided at the top.



Using Qualys search and filter capabilities, you can investigate incidents by the Malware category and by Malware family names.

You can click any Incident Description to view its list of events and other details.

Risk Score of a host incident is based on the highest single event score. If the risk score is zero, then the incident is considered remediated or non-malicious.

**Navigate to the following URL to view the “EDR Incidents” tutorial:**



<https://ior.ad/7Jid>

# Hunt for Suspicious Activity

Adversaries, and cybercriminal organizations in particular, are building tools and using techniques that are becoming so difficult to detect that organizations are having a hard time knowing that intrusions are taking place.

Threat hunting is the proactive technique that's focused on the pursuit of attacks and the evidence that attackers leave behind when they're conducting reconnaissance, attacking with malware, or exfiltrating sensitive data.

Organizations need tools that not only detect and respond to threats, but can proactively hunt them as well. Such tools can accelerate threat discovery to identify a potential compromise before it's too late.

## Hunting Section

The Hunting section provides search and filter capabilities to quickly find all about your incidents, events and assets in one place. You can search for incidents and assets in the respective tabs in the similar way. You'll notice the Search box while viewing dynamic lists of events, incidents, and assets. This is where you'll enter your search query. Enter the value you want to match. As you start typing in the search box, you will see a predefined list of query tokens that you can choose from.

Qualys Cloud Platform

Endpoint Detection and Response

DASHBOARD INCIDENTS **HUNTING** ASSETS RESPONSES

Hunting

523K Total Events

Current View Historic View

Search for events...

Use query tokens to search for specific events or assets

Last 30 Days

TYPE

- file 299K
- mutex 7.96K
- network 6.11K
- process 3.03K
- registry 206K

EVENT ACTION

- created 506K
- established 1.14K
- listening 4.96K
- running 11.0K

SCORE

- 10 5
- 9 64
- 8 987
- 5 16

DETECTED

DETECTED	TYPE	EVENT	ASSET	SCORE	DETAILS	REMEDIATION ACTION
5 days ago 2:29:28 AM	Malicious mutex	\BaseNamedObjects\RasPbFile is created	HC 10	9	Webco... PUA	Kill Process
5 days ago 2:29:28 AM	Malicious mutex	\Sessions\1\BaseNamedObjects\MSCTF.Asm.MutexDefault1 is created	HC 10	9	Webco... PUA	Kill Process
25 days ago 1:23:54 PM	Malicious file	C:\Program Files (x86)\Lavasoft\Web Companion\Application\WebCompanion.e...	IN 10	8	Webco... PUA	Quarantine File
25 days ago 6:40:01 PM	Malicious file	C:\MalwareEXE\2f8e794a-4ffa-11e7-b813-80e65024849a.exe is created	IN 10	8	Rdn Trojan	Quarantine File
25 days ago 6:40:01 PM	Malicious file	C:\MalwareEXE\1e84ff45-414b-11e8-b837-80e65024849a.exe is created	IN 10	8	Agan Trojan	Quarantine File
18 days ago 4:27:54 AM	Malicious file	C:\Users\qualys\Desktop\shadowbroker-master\shadowbroker-master\windows...	HC 10	8	Equatio... Trojan	Quarantine File

1 - 200 of 522788

*EDR online help provides details on the search language and sample queries.*

Once you have your search results you may want to organize them further into logical groupings. Choose a group by option on the left side. You'll see the number of events or assets per grouping. Click on any grouping to update the search query and view the matching events.

Tip - Use your queries to create dashboard widgets on the Dashboards tab.

You can download event search results to your local system you can easily manage incidents or events outside of the Qualys platform and share them with other users. You can export results in CSV format.

## Threat Hunting Queries

Threat hunting is a combination of tools and techniques. Tools can provide information across endpoints; how these tools are used constitute the techniques. Needless to say that any technique you use is only effective with a proper understanding of your own IT environment.

The following examples can be used to identify suspicious activity in your environment.

### Suspicious use of system processes

Service Host ("svchost.exe") is a system process that hosts multiple Windows services. Normal usage is to use the "-k" argument to define the service (via DLL) to instantiate, e.g. "svchost.exe -k imgsvc". This will display the service name that is loaded by svchost. Threat actors try to evade detection by injecting malware directly into svchost.exe instead of calling their code directly, thus there is no "-k" argument. The following query will easily identify such suspicious instances:

```
type: PROCESS and process.name: svchost.exe and action:
RUNNING and not process.arguments: "-k"
```

### System process not running from windows directory

If a file named similar to a system process such as svchost.exe or csrss.exe but is located in a directory other than "C:\Windows\System32\", this indicates that it is not a system file and is malicious. You can identify instances of such system processes not running from their expected locations by using the following query:

```
process.name:svchost.exe and type:process and not
process.fullPath:"C:\Windows\System32\svchost.exe"
```

### PowerShell Execution Bypass

The PowerShell execution policy is the setting that determines which type of PowerShell scripts (if any) can be run on the system. By default it is set to "Restricted", which basically means none. When PowerShell is invoked with the execution bypass argument

nothing is blocked and there are no warnings or prompts. Attackers can use this method to launch PowerShell scripts and evade detection. The following query identifies such PowerShell invocations:

```
type:PROCESS and process.name:powershell.exe and  
process.arguments:"ExecutionPolicy Bypass"
```

#### **PowerShell Obfuscation encoded command**

The attacker could use PowerShell encoded commands in Base64 to obfuscate the malicious activity to evade legacy antivirus and other traditional means of detection. Executing PowerShell scripts with encoded commands could be an indicator of a malicious attack. The following query can be easily used to identify such instances.

```
type:PROCESS and process.name:powershell.exe and  
(process.arguments:"-encodedCommand" or  
process.arguments:"-enc")
```

#### **Process running from Recycle bin or TEMP location**

The \$RECYCLE.BIN has a special purpose in Windows Explorer so items inside of it cannot be interacted with. This does not prevent the executables from being listed as a service, start-up entry, or used from command line. So malware in such locations could be dangerous as well. You can easily identify if any process was launched by a malicious file in the recycle bin as illustrated by this query:

```
process.image.path:Recycle.bin
```

#### **Process with network connection**

Some attackers are writing their malware in Java, a language antivirus software doesn't typically scan for. Java is a common platform in enterprises, and many data centres have it on their white lists, allowing these applications to bypass security controls. Just blocking the Java language isn't typically an option. So tracking suspicious activity involving Java may come in handy to uncover such attacks. The following query identifies any java processes making network connections where the environment may not be configured to allow such an activity:

```
network.process.name:java or network.process.name:jre
```

## **Leverage MITRE ATT&CK Framework**

MITRE ATT&CK defines the tactics, techniques, and procedures that are leveraged by adversaries and malware. MITRE ATT&CK is more behavioral focused that analyzes when humans or malware leverage the built-in operating system binaries, utilities, or capabilities which otherwise might not be malicious on their own.

EDR helps detect malicious behavior on the endpoint by evaluating the events in context with MITRE ATT&CK. Having ATT&CK context also aids analysts when hunting for and responding to incidents within their environment.

Currently, EDR includes the following list of rules as per the MITRE ATT&CK framework to help analyze the events registered on the agents.

- T1053.005 Rule to detect the creation of scheduled task using different binaries listed
- T1090.003 Rule to detect establishment of multi-hop proxy using TOR
- T1098.002 Rule to detect PowerShell process running with argument Add-MailboxPermission
- T1115 Rule to detect PowerShell process running with argument Get-Clipboard
- T1127.001 Rule to detect events where msbuild.exe is running as a child process under given parent process list
- T1201 Rule to detect discovery of password policy using net1.exe binary
- T1218.001 Rule to detect execution of hh.exe binary
- T1218.005 Rule to detect execution of mshta.exe binary
- T1218.009 Rule to detect execution of Regasm/Regsvcs binary
- T1218.011 Rule to detect execution of Rundll32 binary
- T1220 Rule to detect execution of MSXSL binary
- T1569.002 Rule to detect execution of system services using processes listed

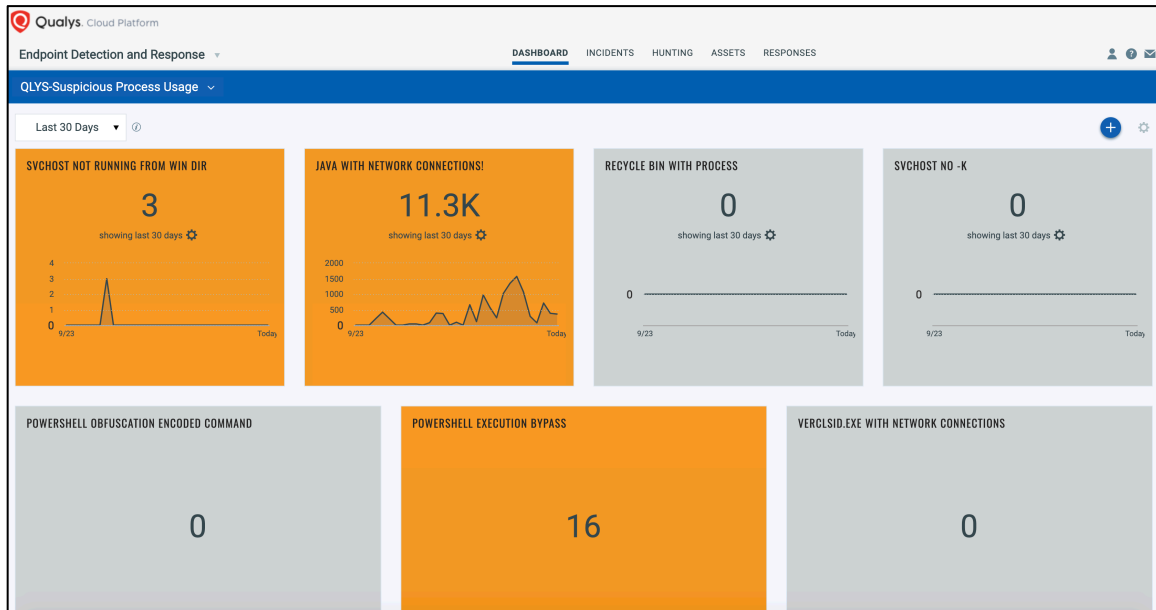
With each release, Qualys continues to add more rules to help classify the events appropriately.

You can use search tokens in the “Hunting” section to search for events by their tactic ID and name and by the technique ID and name in context of MITRE detections.

The applied ATT&CK tactics and techniques are displayed for applicable events on the Event Details page.



# Tracking Threats via Dashboards



Dashboards help you visualize your assets, see your threat exposure, leverage saved searches, and remediate priority of malicious/suspicious events quickly. You can use the default EDR dashboard provided by Qualys or easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also configure widgets to track remediations and to find if a host is getting re-infected over time. You can add as many dashboards as you like to customize your vulnerability posture view.

**Navigate to the following URL to view the “*Hunt for Suspicious Activity*” tutorial:**



<http://ior.ad/7gnT>

# Perform Remediation Action

After data that describes the threat has been collected, the business and technical impact has been identified, and context data has been gathered — remediation can get underway.

## Remediation Actions

You can remediate malicious file events, using the following options:

- **Quarantine File:** Using this option, the file is encrypted and then moved to the Quarantine folder (C:\ProgramData\Qualys\QualysAgent\Quarantine\) on your agent host. The Quarantine folder is automatically created once you upgrade to Cloud Agent version 4.0 for Windows and above.

You can undo this action and restore the file to its original position using the **UnQuarantine File** action from the Responses section, under the User Activity tab.

- **Delete File:** Using this option, the file is permanently deleted from your agent host. You cannot undo this action.
- **Kill Process:** For process, mutex, and network events, we provide Kill Process remediation action. When you perform the Kill Process action for mutex or network events, it kills the corresponding parent process.

Remediation actions can be performed for File, Process, Network, and Mutex events from the Hunting section and from the Event Details page. The remediation options are available only for:

- Events in Active\Current View
- Events that score between 1 to 10

**Navigate to the following URL to view the “Perform Remediation Action” tutorial:**

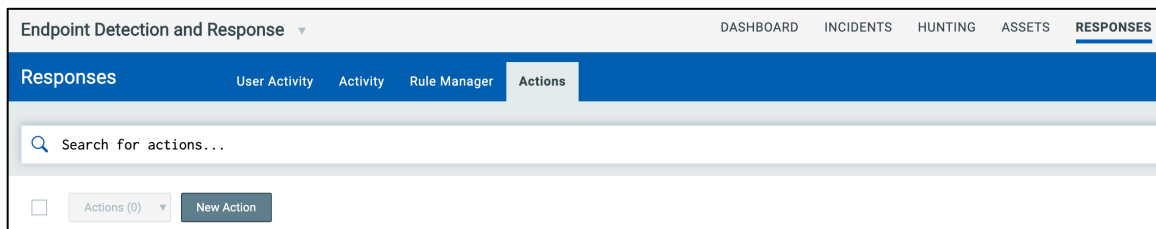


<http://ior.ad/7fLG>

# Configure Rule Based Alerts

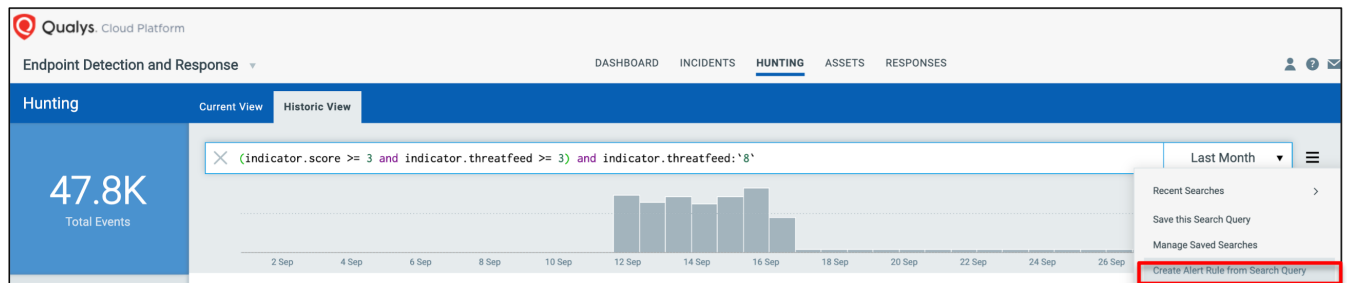
Rule Based alerts provide ongoing detection even after you've completed your hunt, automatically triggering alerts for similar malicious behaviour based on both historical and real-time activity. This eliminates the need to manually search the same security holes over and over by leveraging time-saving automation.

Under the "Responses" section, "Actions" tab you need to first configure a rule Action that will be used with the rule configured in the subsequent step.



Currently, EDR supports three actions: Send Email (Via Qualys), Post to Stack and Send to Pager Duty for alerts.

Next, under "Rule Manager", you need to create a rule with trigger conditions and rule actions for sending the alert. EDR will use the rule action settings to send you the alerts. You can monitor alerts under the "Activity" tab.



You can also create rules directly from custom queries used for searching events or threat hunting as illustrated above.

**Navigate to the following URL to view the "Configure Rule Based Alerts" tutorial:**



<https://ior.ad/7gzK>

# Correlate Prevention Across Multiple Vectors

Multi-vector attacks take advantage of common vulnerabilities, combining elements like social engineering and 'spear phishing' e-mail messages with malicious attachments that contains code that exploits known or unknown (zero-day) vulnerabilities on the target system. While these attacks might rely on commodity malware, they are often tailored to bypass most antivirus engines.

Qualys EDR creates a Single View of the Asset, showing threat hunting details unified with other Qualys Cloud Apps for hardware and software inventory, vulnerability posture, policy compliance controls, and file integrity monitoring change alerts for on-premise servers, cloud instances, and off-net remote endpoints.

A single user interface significantly reduces the time required for incident responders and security analysts to hunt, investigate, detect, and respond to threats before breach or compromise can occur.

With combination of Qualys CyberSecurity Asset Management (CSAM), VMDR, Patch Management (PM) and EDR you can eliminate the root-cause of most malicious attacks by addressing exploitable vulnerabilities and misconfigurations.

## Eliminate Blind Spots

Endpoint security starts with visibility. Qualys CSAM provides you a single source of truth for your assets. It's a central location where you can view your data collected from your different sensors you've deployed. Data collected from your sensors automatically populate into asset inventory. That data is then normalized and categorized so you can better make sense of it and group it in many ways. Because you're getting an inventory, you are completing the first step of the security and compliance teams which is visibility.

CSAM tells what endpoints, servers, technologies you have in your environment. This provides vital context needed for endpoint security and lets you know exactly where EDR can be deployed for eliminating blind spots.

CSAM supports use of elastic queries which helps you quickly identify assets from your infrastructure missing EDR capability.

You can also use dashboard widgets to dynamically track if a critical asset is missing EDR. And you can then tag such assets and activate EDR on them.

## Identify Assets with EOL/EOS Software

Every product has a lifecycle. The lifecycle begins when a product is released and ends when it's no longer supported. When a software reaches end-of-life or EOL, it is no longer sold or marketed by the vendor and it may not receive new feature updates. And when a software hits the end-of-support (EOS) stage, it no longer receives maintenance updates or upgrades from the vendor.

If cybercriminals discover a vulnerability in such EOL/EOS software, there is no guarantee that this vulnerability will be patched by the vendor. Cybercriminals often tend to weaponize such a vulnerability and use it to their advantage.

Timely response to security critical events becomes increasingly important if EOL/EOS and vulnerable software is present within the enterprise environment.

CSAM provides the necessary visibility into the asset and software inventory and into the corresponding lifecycle stages. CSAM also allows you to define software authorization rules to determine what software is allowed or not allowed in your environment, including specific software versions and update levels.

EDR can benefit from this visibility into the asset inventory and software lifecycle information. Security teams benefit from this visibility and they can identify security gaps on critical assets, allowing timely response to contain or eradicate threats and prevent any breach\compromise from spreading across the enterprise infrastructure.

The following query in CSAM identifies Windows assets with EOL/EOS software:

```
operatingSystem:windows and  
software:(lifecycle.stage:EOL/EOS)
```

Going further, you can identify Windows assets that are not enabled for EDR and which have EOL/EOS software of the category "Network Application/ Internet Browser" using the following query:

```
operatingSystem:windows and  
software:((lifecycle.stage:EOL/EOS) and category:`Network  
Application / Internet Browser`) and not  
sensors.activatedForModules:EDR
```

## Identify Vulnerabilities with Malware Associations

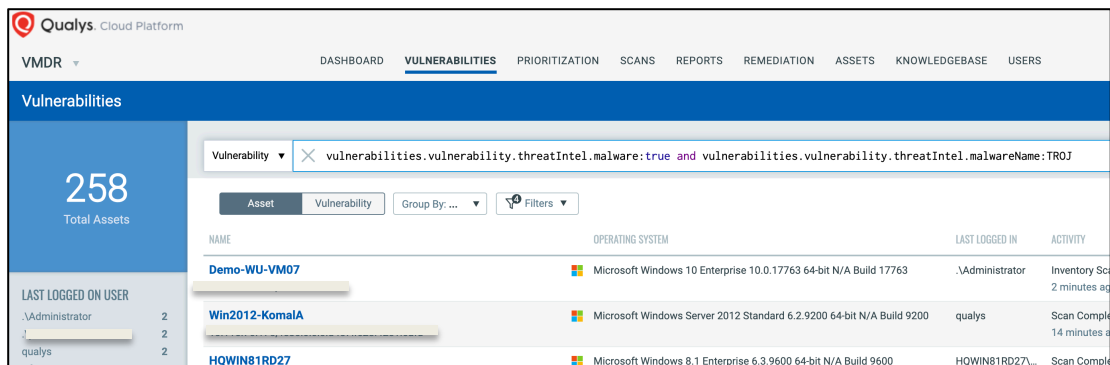
In the "Hunting" tab you can see Incidents related to different malware categories such as trojans, backdoors, exploits and so on.

You can run queries under the "Vulnerabilities" tab in VMDR to easily search for all vulnerabilities linked to the specific malware category.

The following is a sample query to find vulnerabilities linked to the TROJAN malware category:

```
vulnerabilities: threatintel.malware = true and  
vulnerabilities: threatintel.malware.malwarename=TROJ
```

From there, you can identify the assets with such vulnerabilities by simply switching the search result to display asset information.



The screenshot shows the Qualys VMDR interface. The top navigation bar includes DASHBOARD, VULNERABILITIES (selected), PRIORITIZATION, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. The main header is 'Vulnerabilities'. On the left, a sidebar shows '258 Total Assets' and a 'LAST LOGGED ON USER' section with a list of users and their counts. The main content area displays a search bar with the query 'vulnerabilities.vulnerability.threatIntel.malware:true and vulnerabilities.vulnerability.threatIntel.malwareName:TROJ'. Below the search bar, there are tabs for 'Asset' and 'Vulnerability', and a 'Group By' dropdown. The results are shown in a table with columns: NAME, OPERATING SYSTEM, LAST LOGGED IN, and ACTIVITY. The table lists three assets: Demo-WU-VM07 (Microsoft Windows 10 Enterprise), Win2012-Komala (Microsoft Windows Server 2012 Standard), and HQWIN81RD27 (Microsoft Windows 8.1 Enterprise).

NAME	OPERATING SYSTEM	LAST LOGGED IN	ACTIVITY
Demo-WU-VM07	Microsoft Windows 10 Enterprise 10.0.17763 64-bit N/A Build 17763	.Administrator	Inventory Sc 2 minutes ago
Win2012-Komala	Microsoft Windows Server 2012 Standard 6.2.9200 64-bit N/A Build 9200	qualys	Scan Comple 14 minutes ago
HQWIN81RD27	Microsoft Windows 8.1 Enterprise 6.3.9600 64-bit N/A Build 9600	HQWIN81RD27...	Scan Comple

## Identify Vulnerabilities associated with RTIs

VMDR also allows you focus on vulnerabilities that have threats associated with them. These Real-time Threat Indicators or RTIs correlate asset vulnerabilities to external threat vectors such as actively attacked vulnerabilities, wormable threat, zero-days, denial of service attacks, high lateral movement, etc.

By correlating vulnerability information with threat intelligence and asset context, you can quickly “zero in” on your highest risk vulnerabilities and quickly patch them.

The following is a sample query to look for assets with at least one vulnerability that is considered wormable and is known to cause high data loss:

```
vulnerabilities.vulnerability.threatIntel:(wormable:"TRUE"  
and highDataLoss:"TRUE")
```

## Address Vulnerabilities with Patch Management

After identifying assets with exploitable vulnerabilities, you can quickly find out all missing patches for these exploitable vulnerabilities. Then using VMDR’s integrated workflow for Patch Management (PM), you can create a patch job to patch all such vulnerabilities across the environment, which otherwise could have been exploited and

your team would need to put in time to detect, investigate, again correlate and respond to such incidents.

Qualys Cloud Platform

Patch Management

DASHBOARD PATCHES ASSETS JOBS CONFIGURATION

Patch Catalog

4 Total Patches

APP FAMILY

- Windows 3
- Internet Explorer 1

VENDOR

- Microsoft 4

CATEGORY

- Security Patches 3
- Non-Security Pat... 1

Search: Patch qid: [90983,120098] Asset agentId: [1ce6a248-2050-4574-b04b-64967bf7c185,35c9aed3-a783-44ac-8004-6293f3600d28,750018b1-2574-48ea-af1d-aa8133e102c0]

Actions (4) Filters

View Details

Add to Existing Job

Add to New Job

Remove Patch

	ARCHIT	BULLETIN / KB	CATEGORY	QID	VENDOR SEVERITY	MISSING	INSTALLED
up for Server 2012: September 8, 2020 (KB4577038)	X64	MS20-09-MR8-45... KB4577038	Non-Security P...	91413	Critical	1	0
Security Update for Adobe Flash Player: June 9, 2020 (KB4561600)	X64	MS20-06-AFP-456... KB4561600	Security Patch...	370385	Critical	1	0
Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Executio... Published on Aug 11, 2015	X64	MS15-080 KB3078601	Security Patch...	90983	Critical	1	0
Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Executio... Published on Aug 11, 2015	X64	MS15-080 KB3078601	Security Patch...	90983	Critical	1	0

## Identify and Address Misconfiguration

An adversary may identify and exploit weaknesses in the configuration of your infrastructure. These weaknesses could include architectural flaws, misconfigurations, or improper security controls. Searching for failing controls mapped to spread of malware or ransomware or controls mapped to MITRE technique may help identify such misconfigurations and reduce the attack surface.

Combining this context with EDR provides for better threat investigation and assists in fixing misconfiguration that may otherwise lead to malware infections in your environment.

**Navigate to the following URL to view the “Correlate Prevention Across Multiple Vectors” tutorial:**



<https://ior.ad/7fUF>

# EDR Certification Exam

Participants in this training course have the option to take the EDR Certification Exam. This exam is provided through our Learning Management System ([qualys.com/learning](https://qualys.com/learning)).

To take the exam, candidates will need a “learner” account.



Qualys. Training & Certification

[qualys.com/learning](https://qualys.com/learning)

Login

Please log in to the Qualys training site. First time users need to create an account.

\*Required Field

\*Username:

\*Password:

Sign In

Forgot your [password?](#) Request a [new account.](#)

If you would like to take the exam, but do not already have a “learner” account, click the “Request a new account” link, from the “Qualys Training & Certification” login page ([qualys.com/learning](https://qualys.com/learning)).

Once you have created a “learner” account (and for those who already have an account), click the following link to access the “Qualys Multi-Vector Endpoint Detection and Response - QSC 2021” course page:

<https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?&id=22511237811>



**Qualys. Training & Certification**

My Home ▾ Learner Information ▾

**Course Catalog:** Class Details  
Course: Qualys Multi-Vector EDR - QSC 2021

To see how a class below fits into your schedule, click View My Class Schedule.

**CLASS DETAILS: QUALYS EDR - QSC 2021**

**Course Name:** Qualys Multi-Vector EDR - QSC 2021  
**Class Name:** Qualys EDR - QSC 2021  
**Class Code:** 2250729076520210917122310  
**Contact Name:** Vikram Kamat  
**Private Class:** Yes  
**Maximum Class Capacity:** 5000  
**Class Cost:** \$0.00

Session Name ▴	Location	Classroom	Address 1	Address 2	City	State	Postal Code	Times	Instructor(s)
Session 1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Monday, November 15, 2021 9:00 AM to 1:00 PM (America/Los_Angeles) (UTC -07:00)	Vikram Kamat

**Enroll**

From the “Qualys Multi-Vector EDR – QSC 2021” course page, click the “**Enroll**” button (lower-right corner).

After successfully completing the course enrollment, click the “Launch” button, for the Qualys EDR certification Exam.

Class Name	Date	Location	Classroom	Instructor(s)
Qualys EDR - QSC 2021	Monday, November 15, 2021 9:00 AM to 1:00 PM (America/Los_Angeles) (UTC -07:00)	N/A	N/A	Vikram Kamat

To access a learning activity, select the activity name and click Launch or Open.

Activity Name ▴	Type	Score	Progress	Last Accessed	Time Taken	Attempts	Action
QSC 2021 EDR Lab Supplement	pdf	N/A	N/A	N/A	N/A	0	<b>Open</b>
QSC 2021 EDR Slides	pdf	N/A	N/A	N/A	N/A	0	<b>Open</b>
Qualys Endpoint Detection and Response Exam	Actual Test	N/A	Not Attempted	N/A	N/A	N/A	<b>Launch</b>

Each candidate is provided five attempts to pass the exam.

**Print Certificate**

Activities

Class Name	Date	Location	Classroom	Instructor(s)
Qualys EDR - QSC 2021	Monday, November 15, 2021 9:00 AM to 1:00 PM (America/Los_Angeles) (UTC -07:00)	N/A	N/A	Vikram Kamat

To access a learning activity, select the activity name and click Launch or Open.

Activity Name ▴	Type	Score	Progress	Last Accessed	Time Taken	Attempts	Action
QSC 2021 EDR Lab Supplement	pdf	N/A	N/A	N/A	N/A	0	<b>Open</b>
QSC 2021 EDR Slides	pdf	N/A	N/A	N/A	N/A	0	<b>Open</b>
Qualys Endpoint Detection and Response Exam	Actual Test	N/A	Not Attempted	N/A	N/A	N/A	<b>Launch</b>

With a passing score of 75% (or greater), click the “Print Certificate” button to download and print your course exam certificate.